INTERNATIONAL STANDARD

ISO 22320

Second edition
2018-11

Security and resilience — Emergency management — Guidelines for incident management

Sécurité et résilience — Gestion des urgences — Lignes directrices pour la gestion des incidents

Reference number
ISO 22320:2018(E)

Contents

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html.

This document was prepared by Technical Committee ISO/TC 292, *Security and resilience*.

This second edition cancels and replaces the first edition (ISO 22320:2011), which has been technically revised.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html.

Introduction

In recent years, there have been many disasters, both natural and human-induced, and other major incidents which have shown the importance of incident management in order to save lives, reduce harm and damage, and to ensure an appropriate level of continuity of essential societal functions.

Such functions include health, telecommunication, water and food supply, and access to electricity and fuel. While in the past the focus of incident management has been national, regional or within single organizations, today and for the future there is a need for a multinational and multi-organizational approach. This need is driven by relationships and interdependencies between governments, non-governmental organizations (NGO), civil society organizations (CSO) and the private sector internationally.

Factors such as increased urbanization, critical infrastructure dependencies and interdependencies, socio-economic dynamics, environmental change, animal and human diseases and the heightened movement of people and goods around the world have increased the potential for disruptions and disasters that transcend geographic and political boundaries and impact the incident management capability.

This document provides guidance for organizations to improve their handling of all types of incidents (for example, emergencies, crisis, disruptions and disasters). The multiple incident management activities are often shared between organizations and agencies, with the private sector, regional organizations, and governments, have different levels of jurisdiction. Thus, there is a need to guide all involved parties in how to prepare and implement incident management.

Cross-organization-region or -border assistance during incident management is expected to be appropriate to the needs of the affected population and to be culturally sensitive. Therefore, multi-stakeholder participation, which focuses on community involvement in the development and implementation of incident management, is desirable where appropriate. Involved organizations require the ability to share a common approach across geographical, political and organizational boundaries.

This document is applicable to any organization responsible for preparing for or responding to incidents at the local, regional, national and, possibly, international level, including those who

a) are responsible for, and participating in, incident preparation,

b) offer guidance and direction in incident management,

c) are responsible for communication and interaction with the public, and

d) do research in the field of incident management.

Organizations benefit from using a common approach for incident management as this enables collaborative work and ensures more coherent and complementary actions among organizations.

Most incidents are local in nature and are managed at the local, municipal, regional, state or provincial level.

Security and resilience — Emergency management — Guidelines for incident management

1 Scope

This document gives guidelines for incident management, including

— principles that communicate the value and explain the purpose of incident management,

— basic components of incident management including process and structure, which focus on roles and responsibilities, tasks and management of resources, and

— working together through joint direction and cooperation.

This document is applicable to any organization involved in responding to incidents of any type and scale.

This document is applicable to any organization with one organizational structure as well as for two or more organizations that choose to work together while continuing to use their own organizational structure or to use a combined organizational structure.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 22300, *Security and resilience — Vocabulary*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

4 Principles

4.1 General

An organization dealing with any incident should consider the principles described in 4.2 to 4.12.

4.2 Ethics

Incident management respects the primacy of human life and human dignity through neutrality and impartiality.

4.3 Unity of command

Incident management requires that every person at any point in time reports to only one supervisor.

4.4 Working together

Incident management requires organizations to work together.

NOTE For additional information, see Clause 6.

4.5 All-hazards approach

Incident management considers both natural and human induced incidents, including those which the organization has not yet experienced.

NOTE For a definition of all-hazards, see ISO 22300.

4.6 Risk management

Incident management is based on risk management.

NOTE Guidance on risk management is given in ISO 31000.

4.7 Preparedness

Incident management requires preparedness.

4.8 Information sharing

Incident management requires the sharing of information and perspectives.

4.9 Safety

Incident management emphasizes the importance of safety for both responders and those impacted.

4.10 Flexibility

Incident management is flexible (e.g. adaptability, scalability, and subsidiarity).

4.11 Human and cultural factors

Incident management takes human and cultural factors into account.

4.12 Continual improvement

Incident management emphasizes continual improvement to enhance organizational performance.

5 Incident management

5.1 General

Incident management should consider a combination of facilities, equipment, personnel, organizational structure, procedures and communications.

Incident management is predicated on the understanding that in any and every incident there are certain management functions that should be carried out regardless of the number of people who are available or involved in the responding to the incident.

The organization should implement incident management, including

a) an incident management process (5.2), and

b) an incident management structure, which identifies incident management roles and responsibilities, tasks and the allocation of resources (5.3).

The organization should document the incident management process and structure.

5.2 Incident management process

5.2.1 General

The incident management process is based on objectives which are developed by gathering and proactively sharing information in order to assess the situation and identify contingencies.

The organization should engage in planning activities as part of preparedness and response, which consider the following:

a) safety,

b) incident management objectives,

c) information about the situation,

d) monitoring and assessing the situation,

e) planning function which determine an incident action plan,

f) allocating, tracking and releasing resources,

g) communications,

h) relationships with other organizations, common operational picture,

j) demobilization and termination,

k) documentation guidelines.

NOTE 1 Annex D gives recommendations on incident management planning.

NOTE 2 An incident action plan (verbal or written) includes goals, objectives, strategies, tactics, safety, communications and resource management information.

NOTE 3 Demobilize means to return resources to their original use and status.

NOTE 4 Termination means a formal handover from incident management responsibilities to another organization.

Decisions made among organizations should be shared as appropriate. The incident management process applies to any scale of incident (short-/long-term) and should be applied as appropriate to all levels of responsibility. Figure 1 gives a simple example of the incident management process.

The organization should establish an incident management process that is ongoing and includes the following activities:

— observation;

— information gathering, processing and sharing;

— assessment of the situation, including forecast;

— planning;

— decision-making and the communication of the decisions taken;

— implementation of decisions;

— feedback gathering and control measures.

The incident management process should not be limited to the actions of the incident commander but should also be applicable to all people involved in the incident command team, at all levels of responsibility.

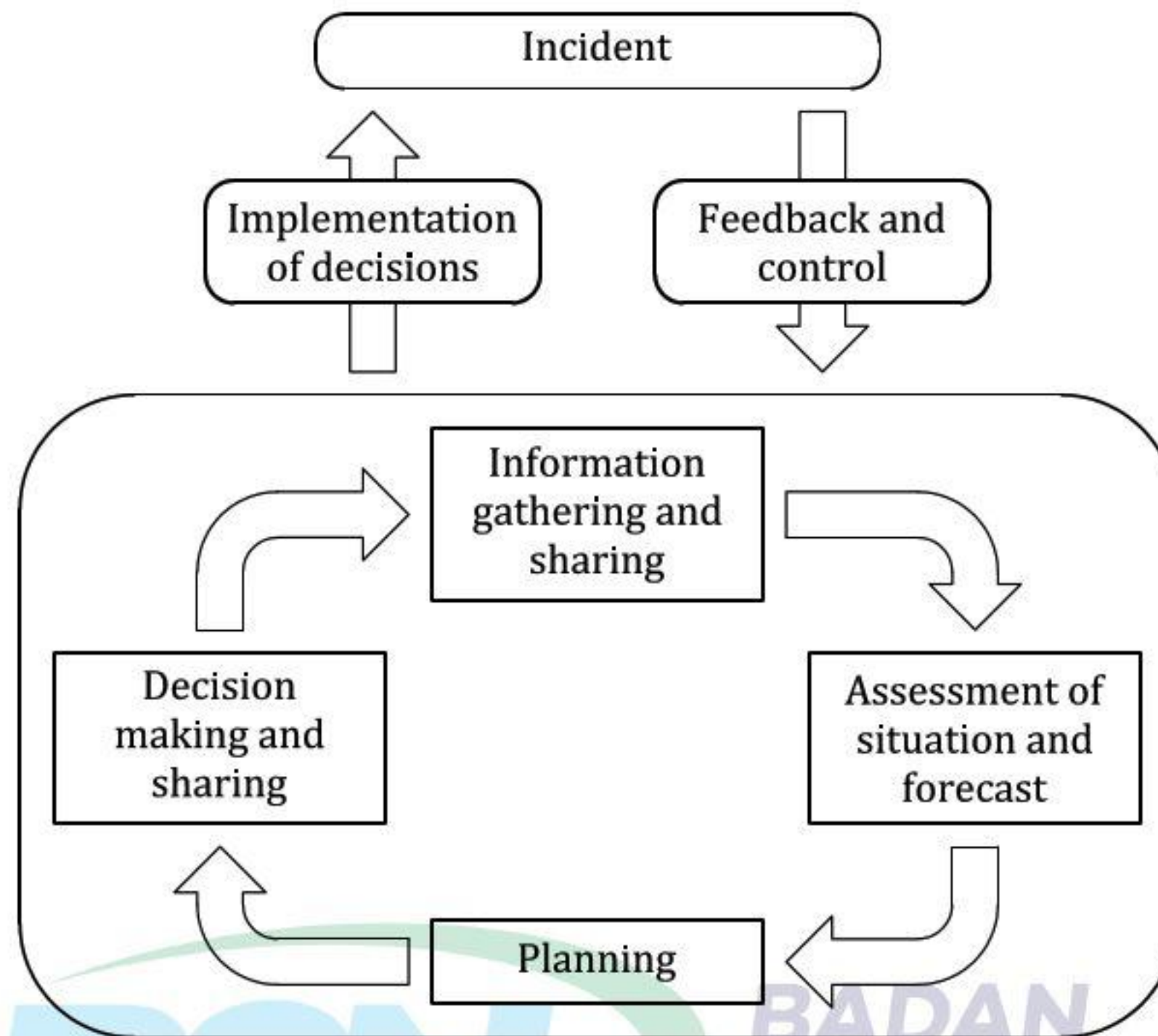



Figure 1 — Incident management process

5.2.2 Different perspectives

The organization should strive to understand other perspectives such as

a) within and outside the organization,

b) various response scenarios,

c) differing needs,

d) various required actions, and

e) different organizational cultures and objectives.

5.2.3 Understanding the importance of time

The organization should

a) anticipate cascading effects,

b) take the initiative to do something sooner, rather than later,

c) consider other organization's timelines,

d) determine the impact of different timelines, and

e) modify its timeline accordingly.

The organization should consider the needs and effects in both the short- and long-term. This includes anticipating

— how the incident will develop,

— when different needs will arise, and

— how long it takes to meet these needs.

5.2.4 Being proactive

The organization should take the initiative to

a) assess risks and align the response to increase response effectiveness,

b) anticipate how incidents can change and use resources effectively,

c) make decisions concerning various measures early enough for decisions to be effective when they are actually needed,

d) manage the incident early,

e) initiate a joint response instead of waiting for someone else to do so,

f) find out what shared information is required, and

g) inform and instruct involved parties, e.g. in order to build up new resources.

5.3 Incident management structure

5.3.1 General

The organization should implement an incident management structure to carry out the tasks relevant to the incident objectives.

An incident management structure should include the following basic functions.

a) Command: authority and control of the incident; incident management objectives structure and responsibilities; ordering and release of resources.

b) Planning: collection, evaluation and timely sharing of incident information and intelligence; status reports including assigned resources and staffing; development and documentation of incident action plan; information gathering, sharing and documentation.

c) Operations: tactical objectives; hazard reduction; protection of people, property and environment; control of incident and transition to recovery phase.

d) Logistics: incident support and resources; facilities, transportation, supplies, equipment maintenance, fuel, food service and medical services for incident personnel; communications and information technology support.

e) Finance and administration: compensation and claims; procurement; costs and time. (Depending on the scale of an incident, a separate financial and administrative function may not be necessary.)

Planning, operations, logistics and finance and administration should be considered for each level of incident management, e.g. sections and subsections of the whole incident management system.

The organization should define and document the minimum staffing requirements to immediately initiate and continuously maintain the organization's incident management.

Annexes B, C and D provide additional information and examples of an incident management structure for one or more collaborating organizations with internal hierarchal structures.

5.3.2 Roles and responsibilities

The organization should clearly define roles and responsibilities of all personnel and the operating procedures to be used. The organization should designate one or more persons with the responsibility for

a) determining incident management objectives,

b) identifying legal and other obligations,

c) initiating, coordinating and taking responsibility for all measures of incident management,

d) establishing the organizational structure, taking span of control into account,

e) assigning tasks, and

f) activation, escalation, demobilization, termination.

Annex C provides additional information.

5.3.3 Incident management tasks

5.3.3.1 At each level of command, the organization should

a) establish incident command and internal organizational structure,

b) assess the risks in the affected area,

c) determine objectives,

d) determine decision-making process,

e) create an action plan,

f) organize the site and develop organizational structure,

g) manage the resources,

h) create a common operational picture,

i) review and modify plans,

j) manage additional facilities,

k) manage additional resources,

l) manage logistics, and

m) keep records.

5.3.3.2 The organization should include the following functions at its top level, as appropriate:

a) safety;

b) public information;

c) liaisons;

d) specific advising/consulting;

e) information and communication technology support.

5.3.3.3 Annex C provides a description of public information and additional examples of incident management tasks.

5.3.3.4 Depending on the scale of the incident, tasks may be combined. In large-scale incidents additional resources may be needed or may be allocated to other organizations. These tasks are also relevant for a joint command in an inter-organizational incident management structure.

5.3.3.5 The organization may allocate responsibility relating to finance and administration, intelligence and investigations to other departments or organizations.

5.3.4 Incident management resources

The organization should administer and manage resources by

a) identifying and quantifying required resources,

b) ordering, tracking and distributing resources, and

c) establishing resource demobilization procedures.

6 Working together

6.1 General

Working together is about coordination and cooperation for both

— different department or levels within a single organization, and

— multiple organizations.

Organizations should use interoperable terminology within the incident management process and structure as described in Clause 5. Additional recommendations are provided in 6.2.2.

NOTE ISO/TR 22351 provides more information on exchange of information.

Organizations should commit to contribute and strive to achieve joint direction. Joint direction results from top management from each organization agreeing on common incident objectives.

Figure 2 and Annex A provide additional information on working together.

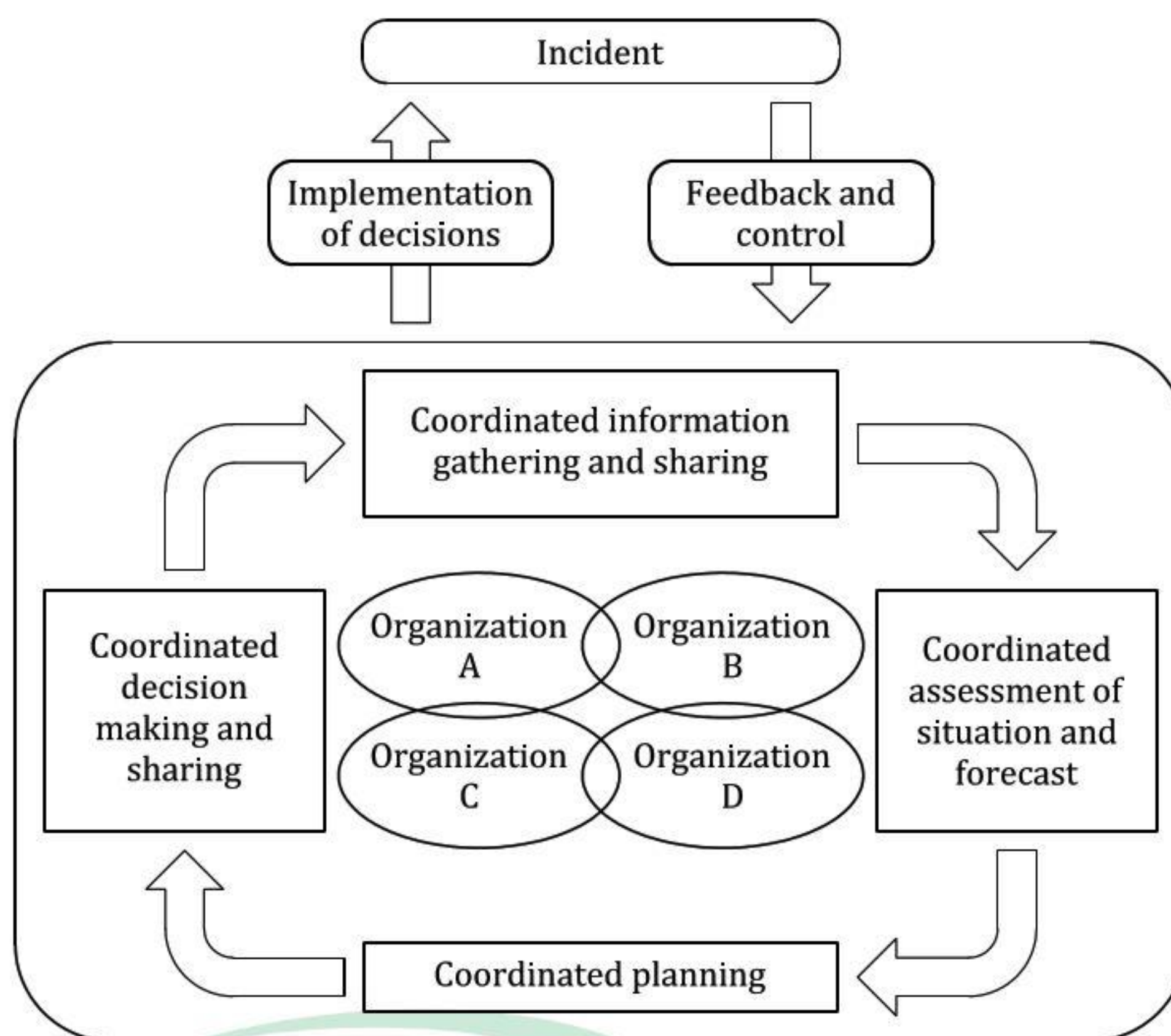



Figure 2 — Coordinated incident management process for multiple organizations

6.2 Prerequisites for achieving coordination and cooperation

6.2.1 Sharing the same incident management process

Working together involves organizations using the incident management process in the same way (see 5.2).

6.2.2 Seeing the whole picture

The organization should look beyond its scope of operations to consider and understand

a) the overall incident management objectives,

b) the other organizations involved and their capabilities,

c) the tasks allocated to other organizations,

d) the resources needed to respond to the incident, and

e) the possible effects of different ways of responding.

6.2.3 Common operational picture

The organization should plan to manage concurrent incidents, as consequences of an incident may arise concurrently on multiple levels and in several sectors of the general public.

When managing concurrent incidents on multiple levels the organization should

— identify the organizations involved in order to avoid duplication and to facilitate the offering of or request for assistance in a timely and simple way,

— anticipate that other organizations may assess the situation in a different way, and

— identify situations (e.g. cascading effects) that may impede or delay agreements and result in inappropriate actions.

The organization should develop a common operational picture by

— actively sharing information with other organizations, ensuring that the requests made are as precise as possible and that the security of information is considered,

— ensuring that information is accessible to other organizations, and

— receiving and analysing information obtained from other organizations.

More information on how to achieve a common operational picture is given in C.6.

6.2.4 Establishing communication

The organization should establish coordinated communication, both within and among organizations, to strengthen credibility, prevent ambiguities and counteract dissemination of incorrect information.

Additional information on collaboration and communication is given in A.5.

6.2.5 Establishing joint decisions

The organization should make decisions together with others based on agreed incident management objectives, be prepared to manage the situation when circumstances change and modify decisions when necessary.

The organization should have a clear and transparent decision-making process, so that decisions are communicated within the organization, to other involved organizations and to the public, where appropriate.

6.3 Developing and implementing methods for working together

6.3.1 General

The organization should

— interpret the development of the incident and its impact on society,

— periodically evaluate the incident management to determine whether the objectives and benefits involving joint activities are being met; use the results of the above evaluations when making joint decisions with regard to continual improvement, and

— conduct training and exercises sufficient to validate the effectiveness of the organization.

6.3.2 Agreements

The organization should establish cooperation agreements with other organizations by

— establishing a dedicated function to ensure coordination, and

— dedicating resources including liaison people.

NOTE ISO 22397 provides additional information for establishing arrangements among organizations.

Cooperation agreements should be established as a part of preparedness where appropriate.

For example, working together is needed between

a) local, regional, national and international authorities concerning mutual assistance,

b) governments on different levels with non-governmental organizations to provide incident management resources (e.g. agreements with radio stations for broadcasting warning and information, general agreements with non-governmental organizations),

c) governments and private industry for incident management support activities (e.g. food, shelter, health services, transportation, communications, delivery of medications, vaccine, emergency power supply capacity and drinking water distribution), and

d) private industry organizations in order to ensure continuity of operations (e.g. delivery of incident management relevant products).

6.3.3 Technical equipment

The organization should use technical equipment to achieve interoperability by

— ensuring equipment functions between organizations and in different environments,

— making the best use of equipment available, and

— considering usage by less-experienced organizations.

Annex A
(informative)

Additional guidance on working together

A.1 Seeing the whole picture

A comprehensive perspective is an approach based on core societal objectives. This means viewing one's own actions as part of a greater whole. This contributes to society's resources being used as efficiently as possible.

An organization with a comprehensive perspective

a) understands how the course of incidents affects the whole of society,

b) understands what needs there are, even those that are outside their own area of responsibility,

c) sees what effects have been achieved or are on their way to being achieved and is able to identify the effects that are lacking, and

d) is able to prioritize if the collective resources are not sufficient to meet all the needs.

Prioritizing is about weighing the various interests linked to the core objectives against each other and giving precedence to that which best satisfies the whole. Which core societal objectives are most pertinent can vary depending on the time and place. As prioritization is always a challenge, the organization should identify in advance what is important in order for society to function.

A.2 Setting different perspectives

Organizations interpret incidents from different perspectives, based on their own missions, operations and capabilities. These different perspectives, contributed by each organization, are important for describing what assistance is needed as comprehensively as possible. Examples of different perspectives are as follows.

a) Every societal organization has its own mission and its own capabilities, as well as its own traditions and ways of looking at how command efforts should be organized.

b) Different organizations may have different mandates and responsibilities.

c) How incidents are viewed by the public also depends on how the details are communicated to them.

Different perspectives, leading to conflict, can stem from at least two sources:

— that the organizations have different interests and therefore want to achieve completely different things;

— that the organizations have different perspectives and look at the problem in different ways.

The organization should develop an understanding of other perspectives and objectives during the planning stage.

A.3 Developing and implementing methods for working together

Organizations that are familiar with other organizational cultures should have trust in others and work better together. However, the management of incidents demands more temporary and spontaneous collaborations. Collaboration in groups can benefit from

— encouraging people to provide viewpoints based on their knowledge and experience,

— working to strengthen the group's cohesion, and

— being watchful of a conformity of thinking.

In work involving more than one organization, individuals, groups and organizations should work towards building up trust in one another. The trust that has been built up can be maintained through

— being able to acknowledge and adapt to other organizations' cultural codes, habits and rituals,

— becoming familiar with and managing power relations, status and hierarchies within the other organization, and

— having an instinctive feel for things that may evoke fear, anger, frustration or shame in others, and controlling one's own emotions.

A.4 Developing and implementing coordination

During incidents time is often a limiting factor. In addition, time becomes more difficult to manage since different aspects of incidents start at different points in time and last for different periods of time. Some incidents may therefore be about to end at the same time as others have not even begun. It is easy to focus on measures that are close together temporally and have a distinct effect, to the detriment of long-term measures.

A.5 Communication

A.5.1 General

Communication aims to create a common and credible reporting of the events of an incident. This takes place between organizations, the general public (including social media) and the media and is an important part of the management of incidents.

Organizations communicate against the background of how the event is reported and perceived by the general public, and partly on the basis of the incident's actual course of events. Organizations should understand how their own message, imagery and perception of reality balance with information from other sources.

Organizations should aim to be as open as appropriate regarding the work each does in incident management. Clear communications by appropriate authorities are a critical and continuous process before, during and after an incident. Prior to an incident, communication objectives focus on public education concerning incident management to enhance awareness of hazards, risks and vulnerabilities; strengthen prevention, mitigation and preparedness measures; and provide information on all aspects of incident management. Public alerting communicates warning messages that a disaster is imminent. Communications during and directly after a disaster explain and guide immediate response actions to minimize impacts and to maintain safety and security. These communications are instructive on the requirements for short-, medium- and long-term recovery.

A.5.2 Establishing communication

The organization should establish and create effective communication coordinated both within and between organizations, to strengthen credibility, prevent ambiguities and counteract the spreading of rumours. The organization should

- make communication skills an integral part of preparedness,
- begin using communication as early as the initial assessment when trying to understand what is happening or has happened,
- collaborate on communication throughout the management of the incident,
- listen to the needs of the target groups and adapt communication accordingly, and
- ensure that communication is characterized by rapidity, openness and accuracy.

All organizations are responsible for the information they provide to the public and the media. In work involving more than one organization, each organization involved has a responsibility to collaborate in order to coordinate information from different organizations, avoid ambiguities and counteract the spreading of rumours.

Annex B
(informative)

Additional guidance on incident management structure

B.1 General

The principles of incident management, coordination and cooperation apply to all organizations, whether they have a single or multiple hierarchical structures. In multiple hierarchical incident management structures the principles of coordination and cooperation are of enhanced relevance.

B.2 Chain of command and unity of command

Chain of command refers to the orderly line of authority within the ranks of the incident management organization. Unity of command means that every individual has a designated supervisor to whom he or she reports at the scene of the incident. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels should be able to control the actions of all personnel under their supervision.

B.3 Joint/unified command

In incidents involving multiple jurisdictions, a single jurisdiction with multiagency involvement, or multiple jurisdictions with multiagency involvement, joint or unified command allows agencies with different legal, geographic, and functional authorities and responsibilities to work together without affecting individual agency authority, responsibility or accountability.

B.4 Span of control

An underlying principle of an incident management is the need to optimize the number of resources being managed by a supervisor in the interest of greater efficiency. This is known as maintaining the "span of control". A normal ratio is one to seven individuals reporting to one person. An optimum span of control consists of two to five individuals reporting to one person. In routine, repetitive environments with lower-risk assignments, or where resources work in very close proximity to each other, it may be acceptable to exceed the recommended span of control. Conversely, in complex incidents where safety is a major factor or where there is a great distance between resources, it is advisable to lower the span of control limit.

B.5 Designated incident facilities

Various types of operational locations and support facilities are established in the vicinity of an incident to accomplish a variety of objectives, such as decontamination, processing of donated goods and evacuation. Typical facilities include incident command posts, bases, camps, staging areas, mass casualty triage areas, incident operations centres and other facilities as required.

B.6 Resource management

Incident management provides processes for categorizing, ordering, dispatching, tracking and recovering resources. In order to ensure readiness, there should be in place, prior to the incident, a standardized, comprehensive database of resources, as well as protocols to access, utilize and demobilize such resources.

Examples of additional expertise and resources that can be considered include

a) human resources, logistics and administrative help to support a sustained response,

b) scientific support (e.g. environmental field monitoring, assurance monitoring),

c) registration and inquiry,

d) incident clothing, shelter and food,

e) transportation,

f) energy supply,

g) pollutant spill response,

h) drinking water,

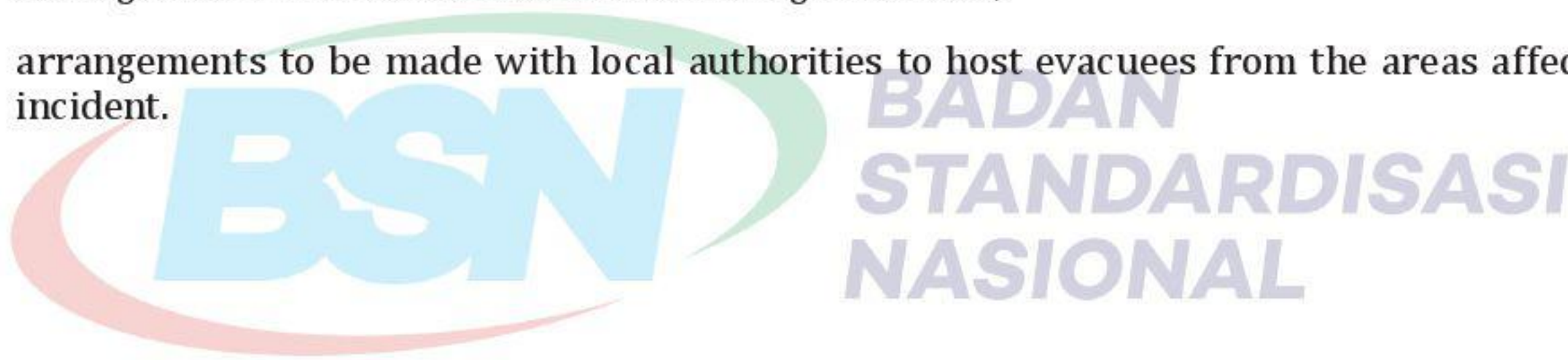
i) health services (e.g. psychological, psychosocial support),

j) worker health and safety, and

k) extraordinary expenditures and compensation.

The organization should also consider the following when managing resources:

— arrangements to be made with volunteer organizations;

— arrangements to be made with local authorities to host evacuees from the areas affected by the incident.

Annex C
(informative)

Examples of incident management tasks

C.1 Incident command

In incident management, the incident command can be an individual or a group responsible for all incident activities, including the development of strategies and tactics and the ordering and the release of resources. The incident command has overall authority and responsibility for conducting incident operations and is responsible for the management of tactical operations at the incident site. The definition of the underlying incident management structures is part of the incident command. The incident command may be supported by a staff.

C.2 Public information

The public information is responsible for interfacing with the public and media and/or with other agencies with incident-related information requirements.

NOTE This task is mostly allocated to the top level of incident command to harmonize the information.

C.3 Liaison officer

The liaison officer is the point of contact for representatives of other governmental agencies, nongovernmental organizations and/or private entities.

C.4 Expert advisor/consultant

Expert advisors/consultants provide specific knowledge from other organizations involved in the emergency response, for example from a science background or with specific professional skills.

C.5 Operations planning and lead

The operations planning and lead is responsible to the incident lead for the direct management of all incident-related operational activities. The operations planning and lead establishes tactics for the assigned operational period and is directly involved in development of any incident management action plan. An operations planning and lead should be designated for each operational period.

C.6 Operational picture

The operational picture provides the collection, evaluation and dissemination of the incident situation information and intelligence for the incident lead and incident management personnel. The operational picture then provides status reports, displays situation information, maintains the status of resources assigned to the incident and documents any incident management action plan, based on the operations planning and lead's input and guidance from the incident lead.

C.7 Logistics

The logistics cover all service support requirements needed to facilitate effective and efficient incident management, including ordering resources from off-incident locations. The logistics also

provides facilities, security (of any incident management command facilities), transportation, supplies, equipment-maintenance and fuel, food services and emergency responder medical services, including inoculations, as required.

C.8 Personnel

As incidents continue, there is a need for organizations to manage personnel accordingly. This includes the scheduling of people and rotating personnel through ongoing operational periods. Other considerations include the needs of personnel communicating with their families.

C.9 Information and communication technology support

The information and communication technology support structures communication, provides secure IT-infrastructure, defines roles and rights for software applications, evaluates the system performances and plans fall back communication and IT structures.

C.10 Finance/administration

A finance/administration is involved when the incident management activities require on-scene or incident-specific finance and other administrative support services. Some of the tasks that fall within this scope are recording personnel time, maintaining vendor contracts, overseeing compensation and claims, and conducting an overall cost analysis for the incident. When a finance/administration is established, close coordination with the planning team and logistics team is also essential so that operational records can be reconciled with financial documents. In addition to monitoring multiple sources of funds, the finance/administration tracks and reports to the incident lead the accrued cost as the incident progresses. This allows the incident lead to forecast the need for additional funds before operations are affected negatively.

C.11 Intelligence and investigations

Intelligence and investigations ensures that all intelligence and investigations operations and activities are properly managed, coordinated and directed in order to

a) prevent and deter potential unlawful activity, incidents or attacks,

b) collect, process, analyse, secure and appropriately disseminate information and intelligence,

c) identify, document, process, collect, create a chain of custody for, safeguard, examine, analyse and store probative evidence,

d) conduct a thorough and comprehensive investigation that leads to the identification, apprehension and prosecution of the perpetrators,

e) serve as a conduit to provide situational awareness (local and national) pertaining to an incident, and

f) inform and support life safety operations, including the safety and security of all response personnel.

NOTE These tasks can be allocated to other organizations that are not necessarily in the line of command (e.g. police).

Annex D
(informative)

Incident management planning

D.1 General

The organization should consider the protection of health, safety, property and the environment as the purpose of the emergency response planning establishment. Incident management plans may be generic or for specific risks, facilities, etc.

When defining the scope of the incident management plan, the organization should consider the following:

a) types of emergencies that are addressed in the plan;

b) types of emergencies that are specifically excluded from the plan (for example, because they are addressed by other plans);

c) responsibilities and limitations due to areas of jurisdiction;

d) scale of emergencies.

The incident management plan should be available in both electronic and hard copy formats during an incident to all organizations identified within the incident management plan.

The incident management plan may be prepared as a stand-alone plan or as an annex to another incident management plan. Even if the incident management plan is stand-alone, it could be integrated with the other incident management plan(s) in the event that the plans are activated concurrently.

D.2 Plan elements

The incident management plan should include, but not be limited to, a number of strategic elements. These elements may include

a) a stated purpose, scope and objectives can be consistent with the defined planning basis and the concept of operations,

b) the complete set of conditions that would require activation of the incident management organization, and the process to activate it,

c) roles and responsibilities,

d) organization and staffing,

e) protective actions and warning systems,

f) interface with and support between response organizations; stakeholder notification, including points of contact that are available at all times,

g) supporting agreements, plans and procedures,

h) communication and information flow,

i) critical facilities and support resources,

j) concept of operations,

k) incident categorization activation and notification; incident assessment; incident classification; predetermined activities for each of the incident categories,

l) continuity of emergency response operations,

m) documentation of decisions and steps taken in response to the emergency, and

n) planning maintenance and administration.

All staff should be informed of and understand their assigned roles and responsibilities in advance of an emergency.

Bibliography

[1] ISO 22324, *Societal security — Emergency management — Guidelines for colour-coded alerts*

[2] ISO/TR 22351, *Societal security — Emergency management — Message structure for exchange of information*

[3] ISO 22397, *Societal security — Guidelines for establishing partnering arrangements*

[4] ISO 31000, *Risk management — Guidelines*